In the Specification:

Please amend the paragraph at page 1, lines 4-11 as indicated below:

The present invention is related to the following commonly-assigned U.S. patents, all of which were filed concurrently herewith: U.S. _____ (Ser. No. ~~09/_____~~) 09/761,906), entitled "Secure Integrated Device with Secure, Dynamically-Selectable Capabilities"; U.S. _____ (Ser. No. ~~09/_____~~) 09/764,844), entitled "Smart Card with Integrated Biometric Sensor"; U.S. _____ (Ser. No. ~~09/_____~~) 09/764,827, entitled "Technique for Continuous User Authentication"; U.S. _____ (Ser. No. ~~09/_____~~) 09/761,899), entitled "Technique for Establishing Provable Chain of Evidence"; and U.S. _____ (Ser. No. ~~09/_____~~) 09/764,541), entitled "Technique for Digitally Notarizing a Collection of Data Streams".

Please amend the paragraph at page 4, lines 3-16 as indicated below:

Let us review the state of the prior art in the field of pervasive computing, as represented by a mobile professional equipped with a collection of the latest generation of specialized personal devices. She may have a cellular telephone, a two-way pager, a "smart" credit card (also known as a "smart card"), a "smart" employee badge used to access secure areas, a PDA, a digital still camera, a digital video camera, a dictation recorder with ~~voice~~ speech recognition capability, an MP3 music player, a remote control key-chain for access to an automobile, a second remote control key-chain for access to a garage, a global positioning system (GPS) navigation aid and map pad, a weather-alert radio, and a personal health alert fob to summon medical aid – all of which may be capable of interacting wirelessly with one another, perhaps via short-range radio technology such as Bluetooth. ("Bluetooth" is a standardized technology that enables devices containing a low-powered radio module to be automatically detected upon coming into radio proximity with one or more other similarly-equipped devices. Devices incorporating this technique are referred to as "Bluetooth-enabled" devices. A standard defining the Bluetooth techniques may be found on the Web at http://www.bluetooth.com.)

Please amend the paragraph at page 8, line 10 to page 9, line 2 as indicated below.

U.S. ~~Patent _____~~, Patent No. 6,772,331, entitled "Method and Apparatus for Exclusively Pairing Wireless Devices", (Ser. No. 09/316,686, filed May 21, 1999) taught a technique for establishing secure trusted relationships between devices in a Bluetooth network using special-purpose hardware, along with software on each device. The special-purpose hardware comprises, for example, a protected memory for storing a digital signature, where this memory is physically attached to the radio transmitter of each device; a display screen on at least one device capable of showing a media access control (MAC) address of the device; and an input button or other comparable device on at least one device for the user to indicate his assent to a trust relationship. While the disclosed technique provides security improvements for networking a collection of devices, there is a significant cost involved. Even if such an investment were made, the overall business process would remain unsecure against certain types of attacks. Furthermore, the disclosed technique cannot be applied to prior art smart credit cards, which have neither a display nor a button for indicating trust.

Please amend the paragraph at page 13, lines 11-20 as indicated below.

In some aspects, transforming the audio stream to a text stream further comprises: transforming the audio stream to a digital stream by a first of the at least one transformation components which is an analog-to-digital transformation component; and converting the digital stream to the text stream by a second of the at least one transformation components which is a ~~voice~~ speech recognition transformation component. In these aspects, digitally notarizing the text stream further comprises: computing a hash over the text stream; combining the hash with unique identifiers of the audio recording component, the analog-to-digital transformation component, and the voice recognition transformation component; and digitally signing the combination using a private cryptographic key of the security core,

wherein the private cryptographic key has a public cryptographic key cryptographically associated therewith.

Please amend the paragraph at page 14, lines 1-18 as indicated below.

In other aspects, transforming the audio stream to a text stream further comprises: transforming the audio stream to a first digital stream by a first of the at least one transformation components which is an analog-to-digital transformation component; converting the first digital stream to a first encoded text stream by a second of the at least one transformation components which is a ~~voice~~ speech recognition transformation component, wherein the ~~voice~~ speech recognition transformation component may be augmented by zero or more others of the at least one transformation components which are an authenticated speaker-specific ~~voice~~ speech recognition database and/or a lexical transformation component; and compressing the first encoded text stream into the text stream using a third of the at least one transformation components which is a text compression transformation component. In this case, digitally notarizing the text stream further comprises: computing a hash over the text stream; combining the hash with unique identifiers of: (1) the audio recording component; (2) the analog-to-digital transformation component; (3) the ~~voice~~ speech recognition transformation component; (4) the authenticated speaker-specific ~~voice~~ speech recognition database and/or the lexical transformation component, if they augmented the ~~voice~~ speech recognition transformation component; (5) the text compression transformation component; and signing the combination using a private cryptographic key of the security core, wherein the private cryptographic key has a public cryptographic key cryptographically associated therewith.

Please amend the paragraph at page 45 lines 7-16 as indicated below.

Furthermore, an optional aspect of the present invention enables such an audio stream to be compressed in a novel manner, from an analog signal to ASCII text (which is arguably the most compact representation of speech). After conversion to digital form, the digital

audio stream is fed into a specific release of ~~voice~~ speech-recognition software for interpretation utilizing a specific release of a vocabulary (possibly augmented by specific speaker-recognition training data, which may be used to enhance the ~~voice~~ speech recognition process). As long as all the devices involved in the data conversion are provably tied to the security core at the time of the data's creation, the resulting notarized signed ASCII text stream, even if not a perfect transcript of the audio portion, could provide a useful and very compressed manner to reliably store evidence of a conversation. Logic which may be used to implement this aspect is provided in Fig. 9.

Please amend the paragraph at page 45, line 17 to page 46, line 7 as indicated below.

As shown at Block 900, an analog data stream containing microphone input is captured, where this microphone has been authenticated using the techniques described with reference to Fig. 2. An identifier for the microphone, referred to in Fig. 9 as "ID1", is provided by the microphone to the security core during the authentication process. This analog data stream is then processed (Block 910) by an analog-to-digital converter, creating a digital data stream. It is assumed that the converter has also authenticated itself to the security core, and established its device identifier as "ID2" in this example. The newly-created digital data stream is then processed by a speaker-specific training database (Block 920) in combination with ~~voice~~ speech recognition software (Block 930) to increase the accuracy of determining the words that have been spoken using knowledge of one or more speaker's speech patterns. (Use of the speaker-specific database may be omitted in some cases.)

Please amend the paragraph at page 46, lines 8-16 as indicated below.

The ~~voice~~ speech recognition software preferably generates an ASCII data stream, referred to in Fig. 9 as "A1". (While the preferred embodiment is described with reference to ASCII data streams, as will be obvious ASCII is merely one type of encoding that may be used. Other data stream encodings, such as EBCDIC or Unicode, may be used alternatively without deviating from the inventive concepts of the present invention.) Optionally, lexical

operations may be performed on this ASCII data stream, such as searching for spelling and/or grammar errors and perhaps performing other types of context-sensitive semantic checks to increase the accuracy of the voice-to-text translation (Block 940). When this type of lexical processing is done, a new ASCII data stream "A2" results.

Please amend the paragraph at page 46, line 18 to page 47, line 9 as indicated below.

It is assumed that the speaker-specific database, ~~voice~~ speech recognition software, and lexical engine (when used) have all authenticated themselves to the security core, according to the present invention, and established their identifiers as "ID3", "ID4", and "ID5". Block 950 then creates a digital notarization for the text stream A2 by signing a hash of a data block containing the identifiers ID1 through ID6 (where "ID6" is the identifier of the authenticated application processor computing the digital signature information) and a hash or checksum of the contents of stream A2, using the security core's private key (in a similar manner to that previously described for creating a digital signature with reference to Fig. 3). This digital notarization may then be stored with the text stream, or alternatively, it may be separately stored. (Note that references herein to hashing data blocks before signing them using public key cryptography is the preferred approach for computing digital signatures for embodiments of the present invention. Alternatively, other methods of signing, such as encrypting the entire block or stream, may be used without deviating from the inventive concepts disclosed herein.)

Please amend the paragraph at page 47, line 16 to page 48, line 2 as indicated below.

Furthermore, the voice characteristics of the speaker(s) may optionally be preserved as annotations in the stream as it is transformed. For example, if an application processor component (such as the ~~voice~~ speech recognition software) deduces the identity of a speaker, then the speaker's name may be included in the text stream prior to (or after, or associated with) the text passages attributed to that speaker. As another option, the annotations might also contain a mathematical summary of the voice characteristics of each speaker, such that

these characteristics could be compared to known samples of speech at a later date to possibly identify the speaker(s).